800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section:	**1. Interoperability Guidelines**	**Status:** Complete
Sub-Section:	**TBD**	
Procedure Title:	**Subscriber Security**	
Date Established:		**SRB Approval:**
Replaces Document Dated:		
Date Revised:	**10/19/2011**	

1. Purpose or Objective

To establish policy & procedures for radio subscriber security, in particular: the management of the "Radio System Keys", which is used for programming subscriber radios with definable security options.

Individual manufacturers of radios have different system key capabilities in managing radio security, so this standard is split into sections based on system key capability.

2. Technical Background:

- **Capabilities**

The system key adds security to Radio programming, and depending on the manufacturer may be programmable with such options as who can program the radio, Radio ID limitations, System ID limitations, and for how long a system key will last before expiring. An Advanced System Key also has the capability of not being copy able, unlike a regular System Key.

Some brands of radios also have the security option of being password protected, which prohibits anyone from reading or modifying the radio without the password.

- **Constraints**

If an advanced system key is used, there is an increased hardware cost, the key itself is a purchasable hardware button, and also requires a reader adapter for the computer.

An advanced system key has a limited life depending on the expiration programmed into the key, and would require replacement as the keys expire. The constraint would be on the financial side, the limited life of the key would be an advantage to the security of the system.

Regular software based system keys "as seen to date", have no time based expiration, so once a key is released, it is permanently active, and more difficult to maintain security on.

3. Operational Context:

The purpose of the system key is to increase the security around the programming of subscriber radios, the details for the management of the keys are defined under sections 4 & 5 of this standard.

If a radio is capable of password protection, this also adds a layer of security to the radio programming, whether this feature is used is entirely up to the individual agencies managing the radios.

4. Recommended Protocol/ Standard:

If a radio is under the responsibility of another administrator, do **NOT** program the radio without the permission of the administrator that is responsible for that radio.

All keys programmed and distributed "software & hardware" will be logged and tracked.

4.a Subsection for radios that are capable of the advanced system key feature:

There are only two master advanced system keys, currently held by MnDOT & Hennepin County, no further master keys will be released to any other agencies.

Agencies having an Advanced System Key can lend their key to 3rd party shops for radio programming, but the agency is responsible for any programming actions performed with the key.

Programmed keys can be updated in all parameters with the exception of the time expiration.

4.b Subsection for radios that are based on the regular software system key feature:

Agencies using a software key are responsible for managing their software key.

A software key can be copied, so precautions will need to be taken to prevent it from being copied, such as not lending the key out, or leaving the key in an unsecured area.

Agencies are not to distribute system keys to other agencies; the software key is only to be used by internal staff of the agency owning the key.

5. Recommended Procedure:

MnDOT holds the Master Advanced System key & software keys, and is the distribution point for system partner agencies and 3rd party service shops, with criteria that the receiving agency has met the requirements of any applicable standards, and has the needed agreements in place to be on the system.

Hennepin County also has a Master Advanced System key, and is grandfathered in for the distribution of the key to internal Hennepin County staff & cities within Hennepin County.

All child keys & software keys programmed will be documented & logged in a tracking spreadsheet located in the As-Built documentation repository.

5.a Subsection for radios that are capable of the advanced system key feature:

Any agency needing an Advanced system key will have to purchase their own key reader & key buttons, and then bring the blank key buttons to MnDOT for programming.

Key expiration will be set to 1 year for 3rd party service shops, and 3 years for system partners.

Key expiration for an unlimited system key will be set to 6 months, and will not be available to 3rd party shops.

Programmed key will be ID range limited to the range(s) needed by the recipient agency for their business needs; ranges can be added / changed as needed by having the key reprogrammed.

A tighter time restriction or other restrictions can be programmed into the distributed keys at the recipient agencies discretion.

5.b Subsection for radios that are based on the regular software system key feature:

Any agency needing a regular software system key will need to contact MnDOT for obtaining a system key.

A software key can be copied, so precautions will need to be taken to prevent it from being copied, such as not lending the key out, or leaving the key in an unsecured area.

6. Management

MnDOT is responsible for the distribution of the System Keys & Advanced System Keys, with the exception of Hennepin County for internal Hennepin County staff operations & cities within Hennepin. Administrators having received a system key / advanced system key are responsible for the management of the key for their respective agency.

Password protection of radios is entirely under individual agencies management & discretion.